MATHEMATICAL COMMUNICATIONS
Math. Commun., Vol. **15**, No. 1, pp. 159-176 (2010)

On unitary splitting perfect polynomials over $\mathbb{F}_{p^2}$

Luis H. Gallardo[1,*] and Olivier Rahavandrainy[1]

[1] *Department of Mathematics, University of Brest 6, Avenue Victor Le Gorgeu, C.S. 93 837, 29 238 Brest Cedex 3, France*

Received March 29, 2009; accepted December 18, 2009

Abstract. We classify some unitary splitting perfect polynomials over a finite field $\mathbb{F}_{p^2}$, where p is a prime number. This generalizes Beard's work over $\mathbb{F}_p$.

AMS subject classifications: 11T55, 11T06, 15A36

Key words: unitary divisors, sum of divisors, polynomials, finite fields, quadratic extensions, circulant matrices

1. Introduction

Let p be a prime number and let $\mathbb{F}_q$ be a finite field of characteristic p with q elements. Let $A \in \mathbb{F}_q[x]$ be a monic polynomial. We say that a divisor d of A is unitary if d is monic and $\gcd(d, A/d) = 1$. Let $\omega(A)$ denote the number of distinct monic irreducible factors of A over $\mathbb{F}_q$ and let $\sigma(A)$ (resp. $\sigma^*(A)$) denote the sum of all monic divisors (resp. unitary divisors) of A (σ and σ^* are multiplicative functions). We denote by $\mathbb{N}$ the set of non-negative integers and by $\mathbb{N}^*$ the set of positive integers. We denote by $\mathbb{R}$ the set of real numbers and by $\mathbb{C}$ the set of complex numbers.

If $\sigma(A) = A$ (resp. $\sigma^*(A) = A$), then we say that A is a perfect (resp. unitary perfect) polynomial. In 1941, E. F. Canaday [4], the first doctoral student of Leonard Carlitz, began the study of perfect polynomials by working on the prime field $\mathbb{F}_2$. Later, in the seventies, J. T. B. Beard Jr. et al. extended this work in several directions (see e.g. [2, 3, 1]). Recently, [6, 7, 8, 9, 11], we became interested in this subject. In our first two papers, we considered the smallest nontrivial field extension of the ground field, namely $\mathbb{F}_4$, while in the three others, (we continued to work on the binary case, by considering "odd" and "even" perfect polynomials we say that a polynomial is *even* (resp. *odd*) over $\mathbb{F}_q$ if it has some root in $\mathbb{F}_q$ (resp. if it is not even)). A polynomial splits over $\mathbb{F}_q$ when all its roots are in $\mathbb{F}_q$. Our first results about splitting perfect polynomials are in [10] and [12], where the fields are respectively $\mathbb{F}_{p^p}$ and $\mathbb{F}_{p^2}$, the Artin-Schreier extension and the quadratic extension of $\mathbb{F}_p$.

Beard [1] was the first to consider splitting polynomials over $\mathbb{F}_p$. First of all, he considered the case of perfect splitting polynomials and then in another paper [2] the case of unitary splitting polynomials.

*Corresponding author. *Email addresses:* Luis.Gallardo@univ-brest.fr (L. H. Gallardo), Olivier.Rahavandrainy@univ-brest.fr (O. Rahavandrainy)

In both cases he succeeded in classyfying these polynomials over $\mathbb{F}_p$. However, his methods are not able to work on more general settings, e.g., when considering the analogous problem over finite extensions of $\mathbb{F}_p$, instead of merely over the prime field $\mathbb{F}_p$.

In our papers (see [10, 12]), we introduced a new method, that uses some linear algebra; more precisely, we use some properties of circulant matrices and more general types of matrices of the same kind (see section 4) to translate some properties of splitting perfect polynomials in properties of these matrices and vice versa. In the present paper we are able to adapt the new method to work also in the case of splitting unitary perfect polynomials. A priori this was not clear since while the unitary perfect polynomials seem by definition simpler than the perfect polynomials, to be able to get results about them is of the same order of difficulty. Indeed, by using our linear algebra method, we discovered (see Theorem 3 and the end of this section) a new family of unitary splitting perfect polynomials over $\mathbb{F}_{p^2}$ without analogue in the classical case of splitting perfect polynomials.

The objective of this paper is to classify some splitting unitary perfect polynomials over $\mathbb{F}_{p^2}$, where p is a prime number (see sections 3 and 4).

For a positive integer m, we consider the set:

$$\Omega_p^m = \begin{cases} \{N \in \mathbb{N} : N \mid p^m - 1\}, \text{ if } p = 2, \\ \{N \in \mathbb{N} : \ 2N \mid p^m - 1\}, \text{ if } p \geq 3. \end{cases}$$

If a splitting polynomial

$$A = \prod_{\gamma \in \mathbb{F}_{p^m}} (x - \gamma)^{h(\gamma)}$$

is unitary perfect over $\mathbb{F}_{p^m}$, then each integer $h(\gamma)$ is of the form $N(\gamma)p^{n(\gamma)}$, where $N(\gamma) \in \Omega_p^m \cup \{0\}$ and $n(\gamma) \in \mathbb{N}$. Moreover, if $h = \min\{h(\gamma) : \ \gamma \in \mathbb{F}_{p^m}, \ h(\gamma) \geq 1\}$, then by Lemma 2, the integer $\text{card}(\{\gamma \in \mathbb{F}_{p^m} : \ h(\gamma) = h\})$ is divisible by p.

Since the product of coprime unitary perfect polynomials is unitary perfect, the following definition is useful for splitting polynomials. We say that A is trivially unitary perfect over $\mathbb{F}_{p^m}$ if it is unitary perfect and if it may be written as a product: $A = A_0 \cdots A_r$, where for each i, j one has

$$\begin{cases} \gcd(A_i, A_j) = 1, \text{ if } i \neq j, \\ \omega(A_i) = p \text{ and } A_i \text{ is unitary perfect of the form: } \prod_{j \in \mathbb{F}_p} (x - \gamma_i - j)^{N_i p^{n_i}}, \\ \gamma_i \in \mathbb{F}_q, \ N_i \in \Omega_p^m, \ n_i \in \mathbb{N}. \end{cases}$$

Note that this definition is slightly different from that of a trivially perfect polynomial in [12]. The case when $q = p$ was already considered by Beard [2]. He showed that a polynomial

$$A = \prod_{\gamma \in \mathbb{F}_p} (x - \gamma)^{N(\gamma)p^{n(\gamma)}}$$

is unitary perfect over $\mathbb{F}_p$ if and only if the following condition holds:

$(\diamond)$: There exist $N, n \in \mathbb{N}$ such that $\forall \ \gamma \in \mathbb{F}_p : n(\gamma) = n, \ N(\gamma) = N \in \Omega_p^1$.

Thus, the only unitary splitting perfect polynomials over $\mathbb{F}_p$ are of the form:

$$(x^p - x)^{Np^n}, \text{ where } n \in \mathbb{N} \text{ and } N \in \Omega_p^1.$$

If $\mathbb{F}_q$ is a nontrivial extension field of $\mathbb{F}_p$, then condition $(\diamond)$ remains sufficient (see again [2]) but not necessary any more (see Theorem 1, in the case $q = 2^2$).

If a splitting polynomial

$$A = \prod_{\gamma \in \mathbb{F}_{p^m}} (x - \gamma)^{N(\gamma)p^{n(\gamma)}}$$

is unitary perfect over $\mathbb{F}_{p^m}$, then two natural cases arise:

Case1: There exists $N \in \mathbb{N}$ such that $\forall\ \gamma \in \mathbb{F}_{p^m} : N(\gamma) = N \in \Omega_p^m$

Case2: There exists $n \in \mathbb{N}$ such that $\forall\ \gamma \in \mathbb{F}_{p^m} : n(\gamma) = n$.

In order to get some progress in the classification of unitary splitting perfect polynomials over a nontrivial extension field of $\mathbb{F}_p$, we work on the smallest nontrivial extension field of $\mathbb{F}_p$, namely the quadratic extension $\mathbb{F}_{p^2}$. If $p = 2$, in Theorem 1 we obtain the list of all splitting unitary perfect polynomials over $\mathbb{F}_4$. We see in particular that Case2 does not imply Case1. If p is odd, we would like to know if Case1 implies Case2. The answer is positive only for some cases (see Theorems 2 and 3).

We fix an algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. We put

$$\mathbb{F}_q = \mathbb{F}_{p^2} = \{j\alpha + i : i, j \in \mathbb{F}_p\} = \mathbb{F}_p[\alpha],$$

where $\alpha \in \overline{\mathbb{F}_p}$ is a root of $\begin{cases} x^2 + x + 1, \text{ if } p = 2, \\ x^2 - c, \qquad c \text{ is not a square in } \mathbb{F}_p \text{ if } p \text{ is odd.} \end{cases}$

If p is odd, we consider the following condition:

$$(\bullet) : N \text{ is even, } N \mid p - 1 \text{ and } \frac{p-1}{N} \text{ is odd.}$$

Observe that condition $(\bullet)$ implies that $2N \nmid p - 1$.

Our main results are the following. Let A be a nonconstant unitary splitting perfect polynomial over $\mathbb{F}_q$. Then A is of the form $A = B^{p^n}$ for some $n \in \mathbb{N}$ where:

a) If $q = 4$:

$$\begin{aligned} &B = (x + d)(x + d + 1),\ d \in \mathbb{F}_4, \\ &B = (x^2 + x)^{2^r}(x^2 + x + 1)^{2^s},\ r, s \in \mathbb{N}, \\ &B = (x^4 + x)^N,\ N \in \{1, 3\}, \\ &B = (x + d)^3(x + d + \alpha)^3\ (x + d + 1)^2(x + d + \bar{\alpha})^2,\ d \in \{0, 1\}, \\ &B = x^3(x + 1)^3\ (x + d)^4(x + d + 1)^6,\ d \in \mathbb{F}_4 \setminus \{0, 1\}. \end{aligned}$$

b) If $q=p^2$, p odd and if $B=\prod_{\gamma\in\mathbb{F}_q}(x-\gamma)^{Np^{n(\gamma)}}$, with $2N \mid q-1$:

B is trivially unitary perfect if $2N \mid p-1$,
$B=(x^q-x)^N$ if $2N \nmid p-1$ and if $(\bullet)$ does not hold,
$B=\prod_{i,j\in\mathbb{F}_p}(x-j\alpha-i)^{N.p^{n_i}}$, $n_i\in\mathbb{N}$ for $i\in\mathbb{F}_p$, if $(\bullet)$ holds.

If we compare our present results to those referring to perfect splitting perfect polynomials given by [6, Theorem 3.4] for $q=4$ and by [12, Theorem 1.1] for $q=p^2$, we see that we essentially obtain analogous results except that in the case of unitary perfectness, there exists an additional family:

$$(x^2+x)^{3.2^n}\ (x+d)^{2^{n+2}}\ (x+d+1)^{3.2^{n+1}}, d\in\{\alpha,\alpha+1\},\ n\in\mathbb{N},\ \text{if } q=4,$$
$$\prod_{i,j\in\mathbb{F}_p}(x-j\alpha-i)^{N.p^{n_i}},\ n_i\in\mathbb{N},\ \text{if } (q=p^2 \text{ is odd, and } N \text{ satisfies } (\bullet)).$$

2. Preliminary

We need the following results. Some of them are obvious, so we omit their proofs. We put $q=p^m$, for some $m\in\mathbb{N}^*$.

Lemma 1. *Let $A=\prod_{\gamma\in\mathbb{F}_q}(x-\gamma)^{h(\gamma)}$ be a unitary perfect polynomial over $\mathbb{F}_q$. Then each integer $h(\gamma)$ is of the form $N(\gamma)p^{n(\gamma)}$, where $N(\gamma)\in\Omega_p^m\cup\{0\}$.*

Proof. The proof is obtained from the following two facts:

- every positive integer h may be written as $h=Mp^v$, where $p\nmid M$ and $v\in\mathbb{N}$.
- any nonconstant polynomial $(x-\gamma)^{Mp^v}+1$ splits over $\mathbb{F}_q$ if and only if $M\in\Omega_p^m$.

□

Lemma 2 (see also [2], Theorem 1)**.** *If $A=P_1^{h_1}\cdots P_r^{h_r}Q_1^{k_1}\cdots Q_s^{k_s}$ is a nonconstant unitary perfect polynomial over $\mathbb{F}_q$ such that:*

$$h_1\deg(P_1)=\cdots=h_r\deg(P_r)<k_1\deg(Q_1)\le\cdots\le k_s\deg(Q_s).$$

Then $r\equiv 0 \pmod p$.

Proof. By definition one has $0=\sigma^*(A)-A=\dfrac{A}{P_1^{h_1}}+\cdots+\dfrac{A}{P_r^{h_r}}+\cdots$
In particular, the leading coefficient of $\dfrac{A}{P_1^{h_1}}+\cdots+\dfrac{A}{P_r^{h_r}}$ equals 0. □

Lemma 3. *Assume that $A=A_1A_2$ is unitary perfect over $\mathbb{F}_q$ and that $\gcd(A_1,A_2)=1$. Then A_1 is unitary perfect if and only if A_2 is unitary perfect.*

Lemma 4. *If $A(x)$ is unitary perfect over $\mathbb{F}_q$, then for any $a \in \mathbb{F}_q$ and for any $n \in \mathbb{N}$, the polynomials $A(x+a)$ and A^{p^n} are also unitary perfect over $\mathbb{F}_q$.*

Remark 1. *If A is a splitting unitary perfect polynomial over $\mathbb{F}_q$, then $\omega(A)$ is not a priori divisible by p. However, by Lemma 2: $\omega(A) \geq p$ if $A \neq 1$.*

Proposition 1. *Let $A = \prod_{j \in \mathbb{F}_p} (x-\gamma_j)^{N_j p^{n_j}}$ be a nonconstant unitary perfect polynomial over $\mathbb{F}_q$, where $N_j \in \Omega_p^m \cup \{0\}$ for all $j \in \mathbb{F}_p$.*
Then:

(i) There exist $N, n \in \mathbb{N}$ such that for each j: $N_j p^{n_j} = N p^n$, $p \nmid N$.

(ii) Moreover, if $2N \mid p-1$, then there exists $\gamma \in \mathbb{F}_q$ such that, after a permutation of indices: $\gamma_j = \gamma + j$, for each $j \in \mathbb{F}_p$.

Proof. i): By Lemma 2, $\omega(A) = p$ and there exists $h \in \mathbb{N}^*$ such that for each j: $N_j p^{n_j} = h = N p^n$ for some $N, n \in \mathbb{N}$, $p \nmid N$.
Now, we may write

$$A = \prod_{j \in \mathbb{F}_p} (x-\gamma_j)^{N p^n}.$$

ii): If $2N \mid p-1$, then there exists $j \in \mathbb{F}_p$ such that $j^N + 1 = 0$. So the monomial $(x-\gamma_0-j)$ divides $\sigma^*((x-\gamma_0)^{N p^n})$ and hence it divides $\sigma^*(A) = A$. Thus, $(x-\gamma_0-j)^{N p^n}$ divides A. By the same argument, the monomial $(x-\gamma_0-lj)^{N p^n}$ divides A, for any $l \in \mathbb{F}_p$. We are done. □

Remark 2. *Part* ii) *of the previous proposition may be false if $2N \nmid p-1$. For example, the polynomial $x^2(x+\alpha)^2(x+2\alpha)^2$ is unitary perfect over $\mathbb{F}_9$, where $\alpha \in \mathbb{F}_9$ is such that $\alpha^2 + 1 = 0$.*

3. Case $\mathbb{F}_4$

We put $\mathbb{F}_4 = \{0, 1, \alpha, \bar{\alpha}\}$, where $\alpha^2 + \alpha + 1 = 0$ and $\bar{\alpha} = \alpha + 1$. We shall use

Lemma 5 (see [6], Lemmas 2.1 and 2.5)**.** *Let $P, Q \in \mathbb{F}_4[x]$ be irreducible and such that $1 + \cdots + P^{2n} = Q^m$ for some $m, n \in \mathbb{N}$, then $n = m = 0$.*

We prove the following result:

Theorem 1. *A splitting polynomial A is unitary perfect over $\mathbb{F}_4$ if and only if it may be written as $A = B^{2^n}$, where $n \in \mathbb{N}$ and B has one of the following forms:*

i) 0,

ii) $(x+d)(x+d+1), d \in \mathbb{F}_4$,

iii) $(x^2+x)^{2^r}(x^2+x+1)^{2^s}, r, s \in \mathbb{N}$,

iv) $(x^4+x)^N, N \in \{1, 3\}$,

v) $(x+d)^3(x+d+\alpha)^3(x+d+1)^2(x+d+\bar{\alpha})^2, d \in \{0, 1\}$,

vi) $x^3(x+1)^3(x+d)^4(x+d+1)^6, d \in \{\alpha, \bar{\alpha}\}$.

Sufficiency is obtained by direct computations. So, we only prove necessity. According to Lemmas 1, 2 and 4, a nonconstant splitting unitary perfect polynomial over $\mathbb{F}_4$ is, after a suitable translation, of the form:

$$A = x^{N.2^n}(x+a)^{N.2^n}(x+b)^{M.2^m}(x+c)^{R.2^r}, \quad a \neq b \neq c,$$

where $a, b, c \in \{1, \alpha, \bar{\alpha}\}, N \in \{1, 3\}, M, R \in \{0, 1, 3\}$ and $n, m, r \in \mathbb{N}$.

We see that A is unitary perfect if and only if:

$$\begin{cases} (E1) : 1 + x^{N.2^n} = (x+a)^{b_1}(x+b)^{c_1}(x+c)^{d_1}, \\ (E2) : 1 + (x+a)^{N.2^n} = x^{a_2}(x+b)^{c_2}(x+c)^{d_2}, \\ (E3) : 1 + (x+b)^{M.2^m} = x^{a_3}(x+a)^{b_3}(x+c)^{d_3}, \\ (E4) : 1 + (x+c)^{R.2^r} = x^{a_4}(x+a)^{b_4}(x+b)^{c_4}, \end{cases} \tag{1}$$

in which the exponents on the sides are non-negative numbers (so that some of them may be zero) and satisfy:

$$\begin{cases} b_1 + c_1 + d_1 = N \cdot 2^n = a_2 + c_2 + d_2 = a_2 + a_3 + a_4 = b_1 + b_3 + b_4, \\ a_3 + b_3 + d_3 = M \cdot 2^m = c_1 + c_2 + c_4, \\ a_4 + b_4 + c_4 = R \cdot 2^r = d_1 + d_2 + d_3. \end{cases} \tag{2}$$

3.1. Case $N = 1$

Subcase $a = 1$: In that case, $x^{2^n}(x+1)^{2^n}$ is unitary perfect. So by Lemma 3, the polynomial $(x+b)^{M.2^m}(x+c)^{R.2^r}$ is also unitary perfect. Hence $b = c + 1 \in \{\alpha, \bar{\alpha}\}$, $M = R \in \{0, 1\}$, $m = r$. We obtain parts i), ii) and iii) of Theorem 1.

Subcase $a \in \{\alpha, \bar{\alpha}\}$: Since α and $\bar{\alpha}$ play symmetric roles, we may suppose that $a = \alpha$, $b = 1$, $c = \bar{\alpha}$. In system (1), we obtain

$$b_3 = d_3,\ a_4 = c_4,\ c_1 = 2^n = d_2,\ b_1 = d_1 = 0 = a_2 = c_2 = 0.$$

Thus system (2) gives

$$\begin{cases} a_3 + a_4 = 2^n, \\ b_3 + b_4 = 2^n, \\ c_4 + 2^n = M \cdot 2^m, \\ d_3 + 2^n = R \cdot 2^r, \\ a_3 + b_3 + d_3 = M \cdot 2^m, \\ a_4 + b_4 + c_4 = R \cdot 2^r. \end{cases}$$

It follows that:

$$M, R \geq 1,\ b_3 = d_3 = R \cdot 2^r - 2^n,\ a_4 = c_4 = M \cdot 2^m - 2^n,\ a_3 = 2^n - a_4 = 2^{n+1} - M \cdot 2^m.$$

So

$$M \cdot 2^m = a_3 + b_3 + d_3 = -M \cdot 2^m + 2R \cdot 2^r.$$

Hence

$$M = R \in \{1, 3\} \text{ and } m = r.$$

If $M = R = 1$, then by equations $(E3)$ and $(E4)$, we have

$$a_3 = 2^m,\ b_3 = d_3 = 0 = a_4 = c_4.$$

Hence $2^n = 2^r = 2^m$ and $r = m = n$.

We obtain part iv) of Theorem 1, with $N = 1$. If $M = R = 3$, then still by equations $(E3)$ and $(E4)$, we have now:

$$a_3 = b_3 = d_3 = 2^m \text{ and } a_4 = b_4 = c_4 = 2^r.$$

Thus:

$$2^n - 2^m = a_4 = 2^r,\ 3 \cdot 2^m - 2^n = c_4 = 2^r, 2^m = d_3 = 3 \cdot 2^r - 2^n.$$

We conclude that $n = m + 1 = r + 1$ and obtain part v) of Theorem 1, with $d = 1$.

3.2. Case $N = 3$

Subcase $a = 1$: We may suppose that $b = \alpha,\ c = \bar{\alpha}$. Moreover, M (resp. m) and R (resp. r) play symmetric roles. In system (1), we obtain the following:

$$b_1 = c_1 = d_1 = 2^n = a_2 = c_2 = d_2,\ a_3 = b_3,\ a_4 = b_4.$$

Thus system (2) gives now:

$$\begin{cases} 2^n + a_3 + a_4 = 3 \cdot 2^n, \\ 2^n + b_3 + b_4 = 3 \cdot 2^n, \\ 2^n + 2^n + c_4 = M \cdot 2^m, \\ 2^n + 2^n + d_3 = R \cdot 2^r, \\ a_3 + b_3 + d_3 = M \cdot 2^m, \\ a_4 + b_4 + c_4 = R \cdot 2^r. \end{cases}$$

It follows that $M, R > 0$ and hence $M, R \in \{1, 3\}$. If $M = R = 1$, then $a_3 = b_3 = 0 = a_4 = b_4$ and we get the contradiction: $2^n = 2^n + a_3 + a_4 = 3.2^n$. If $M = 1,\ R = 3$, then we obtain $a_3 = b_3 = 0$, $a_4 = b_4 = c_4 = 2^r$. Thus, $2^r + 2^n = a_3 + a_4 + 2^n = 3.2^n$ and $2^n + 2^n + 2^r = 2^n + 2^n + c_4 = 2^m$. We get $r = n + 1,\ m = n + 2$. We obtain part vi) of Theorem 1, with $d = \alpha$. If $M = 3,\ R = 1$, then we similarly have $m = n + 1,\ r = n + 2$. We obtain part vi) of Theorem 1, with $d = \bar{\alpha}$. If $M = R = 3$, then we obtain $a_3 = b_3 = d_3 = 2^m$, $a_4 = b_4 = c_4 = 2^r$. Hence $r = m = n$. Thus, we obtain part iv) of Theorem 1, with $N = 3$.

Subcase $a = \alpha$: We may suppose $b = 1$ and $c = \bar{\alpha}$. In system (1), we obtain

$$b_1 = c_1 = d_1 = 2^n = a_2 = c_2 = d_2,\ b_3 = d_3,\ a_4 = c_4.$$

Thus system (2) gives

$$\begin{cases} 2^n + a_3 + a_4 = 3 \cdot 2^n, \\ 2^n + b_3 + b_4 = 3 \cdot 2^n, \\ 2^n + 2^n + c_4 = M \cdot 2^m, \\ 2^n + 2^n + d_3 = R \cdot 2^r, \\ a_3 + b_3 + d_3 = M \cdot 2^m, \\ a_4 + b_4 + c_4 = R \cdot 2^r. \end{cases}$$

It follows that $M, R > 0$ and hence $M, R \in \{1, 3\}$

$$\begin{aligned} a_4 &= c_4 = M \cdot 2^m - 2^{n+1}, \\ b_3 &= d_3 = R \cdot 2^r - 2^{n+1} \\ a_3 &= M \cdot 2^m - R \cdot 2^{r+1} + 2^{n+2}, \\ b_4 &= R \cdot 2^r - M \cdot 2^{m+1} + 2^{n+2}. \end{aligned}$$

If $M = 1$, then by equation $(E3)$, we have $0 = b_3 = d_3 = R \cdot 2^r - 2^{n+1}$ and hence $R = 1,\ r = n + 1$. So by equation $(E4)$:

$$0 = a_4 = c_4 = M \cdot 2^m - 2^{n+1} = 2^m - 2^{n+1}.$$

Thus, $m = n + 1$. We obtain part v) of Theorem 1, with $d = 0$. If $M = 3,\ R = 1$, then we get the contradiction: $0 = a_4 = c_4 = 3.2^m - 2^{n+1}$. If $M = R = 3$, then $a_3 = b_3 = d_3 = 2^m,\ a_4 = b_4 = c_4 = 2^r$. Thus, we get $r = m = n$. We obtain again part iv) of Theorem 1, with $N = 3$.

4. Case $\mathbb{F}_{p^2}$, p odd

A bit of notation is necessary in this section. We put $q = p^2$, where p is an odd prime number.

4.1. Notation

Let $N \in \mathbb{N}$ be a positive integer such that $2N \mid q - 1$. The set of integers $U = \{0, 1, \ldots, p - 1\}$ will also be considered as the prime field $\mathbb{F}_p$. We denote by $\zeta_1, \ldots, \zeta_N \in \mathbb{F}_q$ the N-th roots of -1.
We recall (see the Introduction) that:

$$\mathbb{F}_q = \mathbb{F}_{p^2} = \{j\alpha + i : i, j \in U\} = \mathbb{F}_p[\alpha], \text{ with } \alpha^2 = c \in \mathbb{F}_p,\ \alpha \notin \mathbb{F}_p.$$

We also recall the following condition:

$$(\bullet) : N \text{ is even, } N \mid p - 1 \text{ and } \frac{p-1}{N} \text{ is odd.}$$

Each element $j\alpha + i \in \mathbb{F}_q$ will be, if necessary, identified to the pair $(j, i) \in \mathbb{F}_p \times \mathbb{F}_p$. We define the two following order relations:

- on $\mathbb{F}_p$: $0 \le 1 \le 2 \le \cdots \le p - 1$,
- on $\mathbb{F}_q$ (lexicographic order):

$$(j_0, j_1) \le (l_0, l_1) \text{ if: either } (j_0 < l_0) \text{ or } (j_0 = l_0,\ j_1 \le l_1).$$

For $P, Q \in \mathbb{F}_q[x]$, $P^m \mid\mid Q$ means that $P^m \mid Q$ and that $P^{m+1} \nmid Q$.

For $\gamma \in \mathbb{F}_q$, we put

$$\Lambda^\gamma = \{\delta \in \mathbb{F}_q :\ (\gamma - \delta)^N = -1\} = \{\gamma - \zeta_1, \ldots, \gamma - \zeta_N\}.$$

Observe that:

$$\begin{aligned}\Lambda^\gamma &\neq \emptyset, \text{ if } 2N \mid q-1,\\ \Lambda^\gamma &\subset \{\gamma + j : j \in \mathbb{F}_p\}, \text{ if } 2N \mid p-1,\\ \Lambda^{\gamma+j} &= \{\delta + j : \ \delta \in \Lambda^\gamma\}, \text{ for any } j \in \mathbb{F}_p.\end{aligned}$$

The following straightforward result is useful:

Lemma 6 (see [2], Lemma)**.** *A polynomial Q is unitary perfect if and only if for any irreducible polynomial $P \in \mathbb{F}_q[x]$, and for any positive integers m_1, m_2, we have*

$$(P^{m_1} \mid\mid Q,\ P^{m_2} \mid\mid \sigma^*(Q)) \implies (m_1 = m_2).$$

We obtain an immediate consequence:

Proposition 2. *If $N \geq 1$, then the polynomial $A = \prod_{\gamma \in \mathbb{F}_q} (x-\gamma)^{Np^{n(\gamma)}}$ is unitary perfect if and only if*

$$Np^{n(\gamma)} = \sum_{\delta \in \Lambda^\gamma} p^{n(\delta)}, \ \forall \gamma \in \mathbb{F}_q.$$

Proof. For every $\gamma \in \mathbb{F}_q$, we may apply Lemma 6 to the polynomial $P = x - \gamma$, where $m_1 = Np^{n(\gamma)} \geq 1$. By consideration of:

$$\begin{aligned}\sigma^*(A) &= \prod_{\delta \in \mathbb{F}_q} \sigma^*((x-\delta)^{Np^{n(\delta)}}) = \prod_{\delta \in \mathbb{F}_q} ((x-\delta)^{Np^{n(\delta)}} + 1)\\ &= \prod_{\delta \in \mathbb{F}_q} \prod_{j=1}^{N} (x - \delta - \zeta_j)^{p^{n(\delta)}},\end{aligned}$$

we see that the exponent of P in $\sigma^*(A)$ is exactly the integer $m_2 = \sum_{\delta \in \Lambda^\gamma} p^{n(\delta)}$. Moreover, $m_2 \geq 1$ since Λ^γ is not empty. □

4.2. The results

Let

$$A = \prod_{\gamma \in \mathbb{F}_q} (x-\gamma)^{Np^{n(\gamma)}}$$

be a splitting unitary perfect polynomial over $\mathbb{F}_q$.
Our first main result reads.

Theorem 2. *If $2N \mid p-1$, then A is trivially unitary perfect, so that the integers $n(\gamma)$ may differ.*

Our second main result follows.

Theorem 3. *We have:*

i) If Condition $(\bullet)$ *holds, then:*

$$n(i) = n(\alpha + i) = \cdots = n((p-1)\alpha + i), \text{ for any } i \in U.$$

ii) If $2N \nmid p-1$ *and if Condition* $(\bullet)$ *does not hold, then:*

$$n(\gamma) = n(\delta) := n(say), \text{ for any } \gamma, \delta \in \mathbb{F}_q, \text{ so that } A = (x^q - x)^{Np^n}.$$

As in the case of the splitting perfect polynomials (see [12]), we consider suitable (block) circulant matrices (see [5, Sections 5.6 and 5.8]) to prove our results.

Observe that our method fails if $q = p^m$ with $m \geq 3$, since we cannot apply Lemma 9.

4.3. Circulant matrices

In this section, we recall some results about circulant matrices and block circulant matrices (see [5, Chapters 3 and 4]), that will be useful in the proof of our main results.

Definition 1. *Let* n *be a positive integer. A circulant matrix of order* n *is a square matrix* $C = (c_i^j)_{0 \leq i,j \leq n-1}$ *such that the entries* c_i^j *satisfy*

$$c_i^j = c_{i-1}^{j-1}, \ c_i^0 = c_{i-1}^{n-1}, \text{ for } 1 \leq i, j \leq n-1.$$

Definition 2. *Let* n, m *be positive integers. A block circulant matrix of type* (n, m) *is a square matrix, of order* nm*:* $S = (S_i^j)_{0 \leq i,j \leq n-1}$ *such that*

$$\begin{cases} \text{each matrix } S_i^j \text{ is a square matrix of order } m, \\ S_i^j = S_{i-1}^{j-1}, \ S_i^0 = S_{i-1}^{n-1}, \text{ for } 1 \leq i, j \leq n-1. \end{cases}$$

Furthermore, if every S_i^j *is a circulant matrix, then* S *is called a block circulant with circulant blocks.*

Notation: If C is a circulant matrix of order n and if we denote, for $0 \leq j \leq n-1$:

$$c_j = c_0^j,$$

then C may be written as:

$$C = \operatorname{circ}(c_0, \ldots, c_{n-1}) = \begin{pmatrix} c_0 & c_1 & \ldots & c_{n-1} \\ c_{n-1} & c_0 & \ldots & c_{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ c_1 & c_2 & \ldots & c_0 \end{pmatrix}.$$

Analogously, a block circulant matrix S may be written as:

$$S = \operatorname{bcirc}(S_0, \ldots, S_{n-1}) = \begin{pmatrix} S_0 & S_1 & \ldots & S_{n-1} \\ S_{n-1} & S_0 & \ldots & S_{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ S_1 & S_2 & \ldots & S_0 \end{pmatrix},$$

where $S_j = S_0^j$, for $0 \leq j \leq n-1$.

We will use several times the following result for $n = p$.

Lemma 7 (see [5], Section 3.2)**.** *Let n be a positive integer. Any circulant matrix $C = \mathrm{circ}(c_0, \ldots, c_{n-1})$ is diagonalizable on $\mathbb{C}$, and admits the following eigenvalues:*

$$c_0 + c_1\omega^k + \cdots + c_{n-1}(\omega^k)^{n-1} = \sum_{l=0}^{n-1} c_l(\omega^k)^l, \text{ for } k \in \{0, \ldots, n-1\},$$

where $\omega = \cos(2\pi/n) + i\sin(2\pi/n) \in \mathbb{C}$ is an n-th primitive root of unity.

For the rest of the paper we put

$$\omega = \cos(2\pi/p) + i\sin(2\pi/p) \ \in \ \mathbb{C}.$$

Lemma 8. *Let $j \in U \setminus \{0\}$ and $u_0, \ldots, u_{p-1} \in \mathbb{Q}$ such that*

$$\sum_{r \in U} u_r(\omega^j)^r = 0,$$

then $u_r = u_s$ for any $r, s \in U$.

Proof. Since $\{1, \omega^j, \ldots, (\omega^j)^{p-1}\} = \{1, \omega, \ldots, \omega^{p-1}\}$, we may assume that $j = 1$. It suffices to observe that the cyclotomic polynomial $\Phi_p(x) = 1 + \cdots + x^{p-1}$, which is irreducible, is the minimal polynomial of ω. □

Corollary 1. *Let $C = \mathrm{circ}(c_0, \ldots, c_{p-1})$ be a circulant matrix of order p such that*

$$c_j \neq c_k \text{ for some } j, k \in \{0, \ldots, p-1\}.$$

i) If $\sum_{i=0}^{p-1} c_i = 0$, then 0 is a simple eigenvalue of C.

ii) If $\sum_{i=0}^{p-1} c_i \neq 0$, then 0 is not an eigenvalue of C.

Proof. i): By Lemma 7, C admits the following eigenvalues:

$$c_0 + \cdots + c_{p-1} = 0,$$
$$c_0 + c_1\omega^k + \cdots + c_{p-1}(\omega^k)^{p-1} \neq 0, \text{ for any } k \geq 1, \text{ by Lemma 8.}$$

So, 0 is a simple eigenvalue of C.

ii): By the same argument, 0 is not an eigenvalue of C. So we are done. □

Lemma 9 (see [5], Theorem 5.8.1 and § 2.3)**.** *Let n be a positive integer and let $S = \mathrm{bcirc}(S_0, \ldots, S_{n-1})$ be a block circulant of type (n, n), with circulant blocks, then $S_0, \ldots, S_{n-1}$ are simultaneously diagonalizable on $\mathbb{C}$. Furthermore, a complex number λ is an eigenvalue of S if and only if there exists $k \in \{0, \ldots, n-1\}$ such that λ is an eigenvalue of the circulant matrix $H_k = S_0 + \omega^k S_1 + \cdots + (\omega^k)^{n-1} S_{n-1}$.*

Proof. The fact that $S_0, \ldots, S_{n-1}$ are simultaneously diagonalizable is given by Theorem 5.8.1 in [5]. The same theorem says that the eigenvalues of S are given by the following n matrices:

$$\Upsilon_k = \Gamma_0 + \omega^k \Gamma_1 + \cdots + (\omega^k)^{n-1}\Gamma_{n-1},\ 0 \leq k \leq n-1,$$

where for each $0 \leq j \leq n-1$, the diagonal matrix Γ_j gives the eigenvalues of S_j. It remains to observe, by simultaneous diagonalizability of $S_0, \ldots, S_{n-1}$, that for each k, Υ_k gives the eigenvalues of H_k. □

Corollary 2. *For each $l \in U$, let $S_l = \mathrm{circ}(a_{l,0}, \ldots, a_{l,p-1})$ be a circulant matrix of order p such that:*

$$a_{0,0} \geq 2,\ a_{j,i} \in \{-1, 0\} \text{ if } (j,i) \neq (0,0),\ \sum_{i,j \in U} a_{j,i} = 0 \text{ and } S_m \neq 0 \text{ for some } m \geq 1.$$

Then the following holds.

i) If $H_0 = S_0 + \cdots + S_{p-1} \neq 0$, then H_0 has rank $p-1$.

ii) The matrix $H_k = S_0 + \omega^k S_1 + \cdots + (\omega^k)^{p-1} S_{p-1}$ has rank p, for any $k \geq 1$.

Proof. i): Observe that $H_0 = \mathrm{circ}(t_0, \ldots, t_{p-1})$, where $t_i = \sum_{j=0}^{p-1} a_{j,i}$, for any $i \in U$. If $H_0 \neq 0$, since

$$t_0 + \cdots + t_{p-1} = \sum_{i,j \in U} a_{j,i} = 0,$$

there must exist $j, k \in U$ such that $t_j \neq t_k$. Hence, Corollary 1 implies that 0 is a simple eigenvalue of H_0.

ii): $H_k = \mathrm{circ}(t_{k,0}, \ldots, t_{k,p-1})$, where $t_{k,i} = \sum_{j=0}^{p-1} a_{j,i}(\omega^k)^j$, for any $i \in U$. Since $a_{0,0} \geq 2$ and since $a_{0,1} \in \{-1, 0\}$, we have $a_{0,0} \neq a_{0,1}$. So $t_{k,0} \neq t_{k,1}$, by Lemma 8. The fact that $m \geq 1$ implies that $a_{m,i} \in \{-1, 0\}$ for any $i \in U$. Moreover, since $S_m \neq 0$, there exists $l \in U$ such that $a_{m,l} = -1$. So we get

$$a_{0,0} + a_{0,1} + \cdots + a_{0,p-1} \geq \sum_{i,j \in U} a_{j,i} = 0,$$

and:

$$a_{m,0} + a_{m,1} + \cdots + a_{m,p-1} \leq -1.$$

It follows that: $a_{0,0} + a_{0,1} + \cdots + a_{0,p-1} \neq a_{m,0} + a_{m,1} + \cdots + a_{m,p-1}$, and hence, by Lemma 8:

$$\sum_{i=0}^{p-1} t_{k,i} = \sum_{j=0}^{p-1} (a_{j,0} + a_{j,1} + \cdots + a_{j,p-1})(\omega^k)^j \neq 0.$$

Thus, Corollary 1 implies that 0 is not an eigenvalue of H_k. □

Corollary 3. *Let $S = \mathrm{bcirc}(S_0, \ldots, S_{p-1})$ be a block circulant matrix, with circulant blocks $S_j = \mathrm{circ}(a_{j,0}, \ldots, a_{j,p-1})$, for each $j \in U$. We suppose that:*

$$a_{0,0} \geq 2,\ a_{j,i} \in \{-1, 0\} \text{ if } (j,i) \neq (0,0),\ \sum_{i,j \in U} a_{j,i} = 0 \text{ and } S_m \neq 0 \text{ for some } m \geq 1.$$

Then the following holds.

i) If $H_0 = S_0 + \cdots + S_{p-1} \neq 0$, then S has rank $p^2 - 1$.

ii) If $H_0 = 0$, then S has rank $p^2 - p$.

Proof. i): If $H_0 \neq 0$, then by Corollary 2, H_0 has rank $p-1$ and H_k has rank p for any $k \geq 1$. Hence, by Lemma 9, 0 is a simple eigenvalue of S. So S has rank: $p(p-1) + p - 1 = p^2 - 1$.
ii): By the same argument, if $H_0 = 0$, then 0 is an eigenvalue of S of order p, and the other eigenvalues are not equal to 0. So S has rank: $p(p-1) = p^2 - p$. □

4.4. The proof

For $\gamma \in \mathbb{F}_q$, we put $x_\gamma = p^{n(\gamma)}$. If we identify $\gamma = i\alpha + j$ and $\delta = r\alpha + s$ to the pairs $(i,j),\ (r,s) \in {\mathbb{F}_p}^2$, we may order the unknowns x_{ij} and x_{rs}, as follows:

$$x_{ij} \leq x_{rs} \iff (i,j) \leq (r,s),$$

according to the order relation on $\mathbb{F}_q$ defined in Section 4.1. From Proposition 2, we obtain a linear system of q equations in q unknowns the x_γ's:

$$N x_\gamma = \sum_{\delta \in \Lambda^\gamma} x_\delta,\ \gamma \in \mathbb{F}_q. \tag{3}$$

We denote by S the matrix of that linear system. For $i, j \in \mathbb{F}_p$, we consider the square matrix S_i^j of order p corresponding to the coefficients of unknowns $x_{j\alpha}, x_{j\alpha+1} \ldots, x_{j\alpha+p-1}$, in the p equations:

$$N x_\gamma = \sum_{\delta \in \Lambda^\gamma} x_\delta,\ \text{where } \gamma \in \{i\alpha, i\alpha+1, \ldots, i\alpha+p-1\}.$$

By direct computations, we have the following results:

Lemma 10. *The matrix S can be written as a block matrix:*

$$S = (S_i^j)_{0 \leq i,j \leq p-1},\ \textit{where each } S_i^j \textit{ is a square matrix of order } p.$$

From the definition of Λ^γ, for $\gamma \in \mathbb{F}_q$, we obtain:

Lemma 11. *If $(e_i^j)_{mn}$ is the entry in row m and column n of S_i^j, for $0 \leq m, n \leq p-1$, then:*

$$\begin{cases} (e_i^j)_{mn} = N \text{ if } (j\alpha + n = i\alpha + m), \\ (e_i^j)_{mn} = -1 \text{ if } j\alpha + n \in \Lambda^{i\alpha+m}, i.e\ ((i-j)\alpha + m - n)^N = -1, \\ (e_i^j)_{mn} = 0 \text{ otherwise.} \end{cases}$$

It follows that:

Lemma 12. *One has*

$$\begin{cases} S_i^j = S_{i-1}^{j-1},\ S_i^0 = S_{i-1}^{p-1},\ \text{for } 1 \leq i,j \leq p-1, \\ (e_0^j)_{mn} = (e_0^j)_{m-1\ n-1},\ (e_0^j)_{m0} = (e_0^j)_{m-1\ p-1},\ \text{for } 1 \leq j,m,n \leq p-1. \end{cases}$$

By putting $S_0^j = S_j$, from Lemma 12 we deduce the following two lemmas:

Lemma 13. *The matrix S is a block circulant matrix:*

$$S = \mathrm{bcirc}(S_0, \ldots, S_{p-1}).$$

Lemma 14. *Every matrix $S_j,\ j \in U$, is a circulant matrix of order p:*

$$S_j = \mathrm{circ}((e_0^j)_{00}, \ldots, (e_0^j)_{0p-1}).$$

In the following, for $i,j \in \{0, \ldots, p-1\}$, we put

$$a_{j,i} = (e_0^j)_{0i},\ \text{(the entry in row 0 and column } i \text{ of } S_j).$$

Thus, the matrix S_j becomes

$$S_j = \mathrm{circ}(a_{j,0}, \ldots, a_{j,p-1}).$$

We immediately obtain

Lemma 15. *One has*

i) $a_{0,0} = N$, $a_{j,i} = -1$, *if* $j\alpha + i \in \Lambda^0, a_{j,i} = 0$ *elsewhere;*

ii) $\displaystyle\sum_{(i,j)\in U^2} a_{j,i} = 0;$

iii) $2N$ *divides* $p-1$ *if and only if for any* $j \neq 0,\ S_j = 0.$

Proof. We consider the equation corresponding to $\gamma = 0 = (0,0)$, in the linear system (3). Part i) is obtained by direct computations. ii) is obtained from

$$\sum_{(i,j)\in U^2} a_{j,i} = a_{0,0} + \sum_{\delta \in \Lambda^0} (-1) = N - \mathrm{card}(\Lambda^0) = 0,$$

since Λ^γ contains exactly N elements, for any $\gamma \in \mathbb{F}_q$.
iii): If $2N$ divides $p-1$ and if $j \neq 0$, then for any $i \in \mathbb{F}_p$:

$$a_{j,i} \neq N,\ \text{and } a_{j,i} \neq -1 \text{ since } ((0-j)\alpha + 0 - i)^N \neq -1.$$

Thus, $a_{j,i} = 0$ for any $i \in U$ and $S_j = 0$. We prove the converse by contraposition. If $2N$ does not divide $p-1$, then consider a primitive element β of $\mathbb{F}_q$. We see that $\gamma = \beta^{\frac{q-1}{2N}}$ is of order $2N$. So, we must have: $\gamma^N = -1$. Moreover, $\gamma \notin \mathbb{F}_p$ since $2N \nmid p-1$. We may write: $\gamma = j\alpha + i$ for some $i,j \in \mathbb{F}_p$ such that $j \neq 0$, then $a_{j,i} = -1$. Hence $S_j \neq 0$. □

If p is odd, by ℓ we denote the order of c in $\mathbb{F}_p$, so that α is of order 2ℓ in $\mathbb{F}_q$. Without loss of generality, we may assume c to be a primitive element, and hence $\ell = p-1$. We consider then the following condition:

$$(\bullet\bullet) : N \text{ is even and } x^N + c^{-\frac{N}{2}} \text{ splits in } \mathbb{F}_p.$$

Corollary 4. *We have $S_0 + \cdots + S_{p-1} = 0$ if and only if Condition $(\bullet\bullet)$ holds.*

Proof. Necessity: Firstly, $S_0 + \cdots + S_{p-1} = 0$ if and only if for each $i \in U$,

$$\sum_{j=0}^{p-1} a_{j,i} = 0.$$

So by Lemma 15, $a_{j,i} = 0$ for any $i \geq 1$. Moreover, since $a_{0,0} = N$, there must exist distinct $j_1, \ldots, j_N \in \mathbb{F}_p$ such that:

$$a_{j_1,0} = \cdots = a_{j_N,0} = -1, \text{ and } a_{j,0} = 0, \text{ for any } j \notin \{j_1, \ldots, j_N\}.$$

Hence, for each $1 \leq l \leq N$, we have $(-j_l\ \alpha)^N = -1$. It follows that $\alpha^N \in \mathbb{F}_p$ so that N must be even. Moreover, for any $l \in \{1, \ldots, N\}$:

$$({j_l}^N + c^{-\frac{N}{2}})\ c^{\frac{N}{2}} = {j_l}^N \alpha^N + 1 = (-j_l\alpha)^N + 1 = 0.$$

Hence, $j_1, \ldots, j_N$ are the roots in $\mathbb{F}_p$ of the polynomial: $x^N + c^{-\frac{N}{2}}$.
Sufficiency: Let $j_1, \ldots, j_N \in \mathbb{F}_p$ be the roots of $x^N + c^{-\frac{N}{2}}$. For each $1 \leq l \leq N$, we have:

$$(-j_l\ \alpha)^N = {j_l}^N\ \alpha^N = -c^{-\frac{N}{2}}\alpha^N = -1.$$

Hence, for any $(j,i) \notin \{(j_1,0), \ldots, (j_N,0)\}$, $(-j\ \alpha - i)^N \neq -1$ so that $a_{j,i} = 0$. □

We recall that $(\bullet)$ denotes: N is even, $N \mid p-1$ and $\dfrac{p-1}{N}$ is odd.
Observe that

Proposition 3. *Condition $(\bullet)$ is equivalent to Condition $(\bullet\bullet)$.*

Proof. Necessity: Put $\dfrac{p-1}{N} = M$ odd. If $u \in \overline{\mathbb{F}_p}$ satisfies: $u^N + c^{-\frac{N}{2}} = 0$, then

$$u^{p-1} = (u^N)^M = (-1)^M\ c^{-\frac{NM}{2}} = (-1)\ c^{-\frac{p-1}{2}} = 1,\ c \text{ not being a square.}$$

Thus, $u \in \mathbb{F}_p$. So the polynomial $x^N + c^{-\frac{N}{2}}$ splits over $\mathbb{F}_p$.
Sufficiency: It is clear that N is even. Now, we prove that N divides $p-1$.
If $j_1, \ldots, j_N \in \mathbb{F}_p$ are the roots of $x^N + c^{-\frac{N}{2}}$, then $(j_l/j_1)^N = 1$, for any $l \in \{1, \ldots, N\}$. So the polynomial $x^N - 1$ splits in $\mathbb{F}_p$. Since $p \nmid N$, we conclude that $N \mid p-1$. It remains to show that $M = p-1/N$ is odd. By hypothesis, any root u of $x^N + c^{-N/2}$ lies in $\mathbb{F}_p$, so that $u^{p-1} = 1$. Hence, since c is not a square, we have

$$1 = u^{p-1} = (u^N)^M = (-1)^M\ c^{-\frac{NM}{2}} = (-1)^M c^{-\frac{p-1}{2}} = -(-1)^M.$$

We are done. □

4.4.1. Proof of Theorem 2

Lemma 16. *If $2N \mid p-1$, then S_0 has rank $p-1$ and S is the block diagonal matrix:*

$$S = \mathrm{bcirc}(S_0, 0, \dots, 0) = \mathrm{diag}(S_0, \dots, S_0).$$

Proof. The rank of S_0 is obtained by Corollary 1. By Lemma 15- iii), $S_j = 0$ for all $j \in U \setminus \{0\}$, so that $S = \mathrm{diag}(S_0, \dots, S_0)$. □

Corollary 5. *If $2N \mid p-1$, then $n(\gamma) = n(\gamma+1) = \cdots = n(\gamma+p-1)$, for any $\gamma \in \mathbb{F}_q$.*

Proof. By Lemma 16, the matrix S is exactly the diagonal matrix $\mathrm{diag}(S_0, \dots, S_0)$, so the linear system (3) splits into p linear systems (each of which is of matrix S_0) in p unknowns $x_\gamma, x_{\gamma+1}, \dots, x_{\gamma+p-1}$:

$$N x_{\gamma+j} = \sum_{\delta \in \Lambda^{\gamma+j}} x_\delta, \text{ for } \gamma = i\alpha,\ i, j \in \mathbb{F}_p. \tag{4}$$

Moreover, S_0 has rank $p-1$. It remains to observe that $(1, \dots, 1)$ belongs to the kernel of S_0, since

$$a_{0,0} + \cdots + a_{0,p-1} = \sum_{i \in U} a_{0,i} + 0 = \sum_{i \in U} a_{0,i} + \sum_{i,j \in U, j \neq 0} a_{j,i} = \sum_{(i,j) \in U^2} a_{j,i} = 0,$$

by Lemma 15 ii). □

4.4.2. Proof of Theorem 3

In this subsection, we suppose that $2N$ does not divide $p-1$. So, by Lemma 15 iii), there exists $m \geq 1$ such that $S_m \neq 0$. Moreover, $a_{0,0} = N \geq 2$. Corollaries 3 and 4, and Proposition 3 give

Proposition 4. *One has*

If Condition (•) holds, then the matrix S has rank $p^2 - p$.

If Condition (•) does not hold, then the matrix S has rank $p^2 - 1$.

We obtain now Theorem 3:

Corollary 6. *One has*

i) If Condition (•) holds, then:

$$n(i) = n(\alpha + i) = \cdots = n((p-1)\alpha + i), \text{ for any } i \in U.$$

ii) If (•) does not hold, then $n(\gamma) = n(\delta)$ for any $\gamma, \delta \in \mathbb{F}_q$.

Proof. i): In this case, the matrix S has rank $p^2 - p = q - p$, so its kernel $Ker(S)$ is of rank p. Now, consider $v = (x_{0,0}, x_{0,1}, \ldots, x_{0,p-1}) \in \mathbb{R}^p$ and its transpose $v^\top$. Since $S = \text{bcirc}(S_0, S_1, \ldots, S_{p-1})$ with $S_0 + \cdots + S_{p-1} = 0$, we get

$$S \cdot \begin{pmatrix} v^\top \\ v^\top \\ \vdots \\ v^\top \end{pmatrix} = \begin{pmatrix} S_0 \cdot v^\top + S_1 \cdot v^\top + \cdots + S_{p-1} \cdot v^\top \\ S_{p-1} \cdot v^\top + S_0 \cdot v^\top + \cdots + S_{p-2} \cdot v^\top \\ \vdots \\ S_1 \cdot v^\top + \cdots + S_{p-1} \cdot v^\top + S_0 \cdot v^\top \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Hence, $Ker(S)$ contains the vector space E of dimension p:

$$\begin{aligned} E &= \{(v, \ldots, v) \in (\mathbb{R}^p)^p : v = (x_{0,0}, x_{0,1}, \ldots, x_{0,p-1}) \in \mathbb{R}^p\}, \\ &= \{(x_{0,0}, \ldots, x_{j,i}, \ldots, x_{p-1,p-1}) \in \mathbb{R}^q : x_{0,i} = \cdots = x_{p-1,i},\ \forall\, i \in U\}. \end{aligned}$$

We are done.
ii): Here, the matrix S has rank $p^2 - 1 = q - 1$. Furthermore, $(1, \ldots, 1)$ belongs to the kernel of S, since

$$\sum_{(i,j) \in U^2} a_{j,i} = 0,$$

by Lemma 15 ii). □

Acknowledgments

We are grateful to the referee for his observations. The result is an improved paper.

References

[1] J. T. B. Beard Jr., J. R. O'Connell Jr., K. I. West, *Perfect polynomials over $GF(q)$*, Rend. Accad. Lincei **62**(1977), 283–291.
[2] J. T. B. Beard Jr., *Unitary perfect polynomials over $GF(q)$*, Rend. Accad. Lincei **62**(1977), 417–422.
[3] J. T. B. Beard Jr., *Perfect polynomials Revisited*, Publ. Math. Debrecen **38**(1991), 5–12.
[4] E. F. Canaday, *The sum of the divisors of a polynomial*, Duke Math. J. **8**(1941), 721–737.
[5] P. J. Davis, *Circulant Matrices*, Chelsea Publishing New York, New York, 1979. (Reprinted 1994.)
[6] L. Gallardo, O. Rahavandrainy, *On perfect polynomials over $\mathbb{F}_4$*, Port. Math. (N.S.) **62**(2005), 109–122.
[7] L. Gallardo, O. Rahavandrainy, *Perfect polynomials over $\mathbb{F}_4$ with less than five prime factors*, Port. Math. (N.S.) **64**(2007), 21–38.
[8] L. H. Gallardo, O. Rahavandrainy, *Odd perfect polynomials over $\mathbb{F}_2$*, J. Théor. Nombres Bordeaux **19**(2007), 165–174.
[9] L. H. Gallardo, O. Rahavandrainy, *Even perfect polynomials over $\mathbb{F}_2$ with four prime factors*, Int. J. Pure Appl. Math. **52**(2009), 301–314.
[10] L. H. Gallardo, O. Rahavandrainy, *On splitting perfect polynomials over $\mathbb{F}_{p^p}$*, preprint.

[11] L. H. GALLARDO, O. RAHAVANDRAINY, *There is no odd perfect polynomial over* $\mathbb{F}_2$ *with four prime factors*, Port. Math. (N.S.) **66**(2009), 131–145.
[12] L. H. GALLARDO, O. RAHAVANDRAINY, *On splitting perfect polynomials over* $\mathbb{F}_{p^2}$, Port. Math. (N.S.) **66**(2009), 261–273.